Indiana Intelligence Fusion Center

Face Recognition Policy

June 1, 2018

The Indiana Intelligence Fusion Center Face Recognition Policy represents the privacy policy applicable to all IIFC operations and activities.

Table of Contents

{Page intentionally left blank}

Indiana Intelligence Fusion Center (IIFC) Face Recognition Policy

Purpose Statement

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons. The **Indiana Intelligence Fusion Center** has implemented a face recognition program to support the investigative efforts of law enforcement and public safety agencies both within and outside the State of Indiana.

It is the purpose of this policy to provide Indiana Intelligence Fusion Center personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes.

Further, this policy will delineate the manner in which requests for face recognition are received, processed, catalogued, and responded to.

This policy assists the Indiana Intelligence Fusion Center and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

All deployments of the face recognition program are for official law enforcement sensitive (LES). The provisions of this policy are provided to support the following authorized uses of face recognition information:

- Reasonable suspicion exists that the subject of the criminal intelligence information is involved with or has knowledge of possible criminal or terrorist activity; and
- The criminal intelligence information is relevant to the criminal or terrorist activity.

Policy Applicability and Legal Compliance

The policy is applicable to all personnel working in direct support of the IIFC.

The image was not obtained in violation of applicable federal, state, or local laws or ordinances (delegable to a submitting agency), including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the Indiana Intelligence Fusion Center.

An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if:

- The outside agency is a law enforcement agency or provides a law enforcement function that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in the IIFC Privacy Policy. The requestor shall provide their contact

information (requestor's name, requestor's agency, address, and phone number), and lawful reason for request.

The IIFC shall provide the following statement to any identification provided to the requestor:

- *The result of a face recognition search is provided by the Indiana Intelligence Fusion Center only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.*

Governance and Oversight

Primary responsibility for the operation of the IIFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Executive Director of the IIFC.

The Indiana Intelligence Fusion Center Executive Director will be responsible for the following**:**

- Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.

The Indiana Intelligence Fusion Center face recognition program was established on January 1, 2018 in conjunction with the Indiana State Police. Personnel from the following agencies are authorized to request face recognition searches:

- Any Federal, State, Local, Tribal or governmental agency acting in a law enforcement capacity and making a lawful request or providing a lawfully obtained image for face recognition analysis under the guidelines of the IIFC Privacy Policy of this document.

The Indiana Intelligence Fusion Center contracts with Vigilant Solutions to provide software and system development services for the Indiana Intelligence Fusion Center face recognition system. The Indiana Intelligence Fusion Center retains ownership rights to the face recognition system and the images and information it contains.

IIFC privacy compliance is guided by a trained Privacy Officer who is appointed by the Executive Director. Violations of the privacy policy can be reported to, the Executive Director, Assistant Director or to the Privacy Officer. Reporting can be made in person, written or via any electronic communication.

Acquiring and Receiving Face Recognition Information

The Indiana Intelligence Fusion Center (IIFC) is authorized to access and perform face recognition searches utilizing the following external repositories:

- Mug-shot images via the Indiana State Police Criminal Justice Data Division
- Vigilant Solutions general image file
- Open source images

For the purpose of performing face recognition searches, the IIFC and authorized IIFC personnel will obtain probe images or accept probe images from authorized requesting or participating agencies only for the authorized uses identified in the IIFC Privacy Policy.

Use of Face Recognition Information

The IIFC does not connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face recognition system will not be configured to conduct face recognition analysis on live or recorded video.

The following describes the Indiana Intelligence Fusion Center's (IIFC) manual face recognition search procedure, which is conducted in accordance with the IIFC Privacy Policy and this policy.

- Federal, State, Local law enforcement personnel will submit a probe image of a subject of interest.
- Trained IIFC analysts will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository.
- In the automated search, most likely candidates are returned to the analyst to analyze for confidence. The resulting candidates, if any, are then manually compared with the probe images and examined by an analyst. Analysts shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.
    - If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the analyst will not be provided to the requesting entity.
- Analysts should submit the search and subsequent examination results for a peer review of the probe and candidate images for verification by other analysts.
- All entities receiving the results of a face recognition search, must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation.

Sharing and Disseminating Face Recognition Information

The Indiana Intelligence Fusion Centers (IIFC) face recognition search information will not be:

- Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the IIFC's agreement with the commercial vendor.
- Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the IIFC and the originating agency may agree in writing in advance that the IIFC will disclose face recognition search information as part of its normal operations, including disclosure to an external auditor of the face recognition search information.
- Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the IIFC and the originating agency.
- Disclosed to unauthorized individuals or for unauthorized purposes.

Data Quality Assurance

- Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.
- IIFC analysts will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.
- The IIFC considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only. Face recognition search results are **not** considered positive identification of a subject and do not, on their own, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

The IIFC will make every reasonable effort to perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:

- Personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
- Malfunctions or deficiencies of the system will be reported to the Director of Operations upon discovery of the malfunctions or deficiencies.

The integrity of information depends on quality control and correction of recognized errors which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The IIFC will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The IIFC will correct the information or advise the process for obtaining correction of the information.

Disclosure Requests

Face recognition information will only be disclosed to the public in accordance with IIFC's privacy policy.

Security and Maintenance

- The IIFC will comply with generally accepted industry or other applicable standards for security, in accordance with Indiana Office of Technology to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related IIFC activity.
- All entities to the project will operate in a secure environment protected with multiple layers of security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Any access to IIFC face recognition information from outside the facility will be allowed only over secure networks.
- All results produced by the IIFC as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.
- All face recognition equipment and face recognition software and components will be properly maintained in accordance with the manufacturer’s recommendations, including routine updates as appropriate.
- The IIFC and contributing entities will store face recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.
- Authorized access to the IIFC face recognition system will be granted only to personnel whose positions and job duties require such access.
- Usernames and passwords to the face recognition system are not transferrable, must not be shared by IIFC personnel, and must be kept confidential.
- Queries made to the IIFC’s face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
- The IIFC will maintain an audit trail of requested, accessed, searched, or disseminated IIFC held face recognition information, via Vigilant Solutions. An audit trail will be kept for requests, access, and searches of face recognition information for specific purposes and of what face recognition information is disseminated to each individual in response to the request.

Information Retention and Destruction

- All images utilized by the IIFC, via the Indiana State Police Criminal Justice Data Division, will be stored for a period determined by the Indiana State Police Criminal Justice Data Division.
- Once a face recognition image is downloaded by IIFC personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information, and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.
- Any images that do not originate with the IIFC will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency. Images provided by an agency will be considered lead information and retained per the IIFC privacy policy pertaining to lead information, until such time that the originating agency provides an update to IIFC.
- The IIFC retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the IIFC subject to applicable legal requirements.

- Probe images are stored in an analyst working file for only as long as needed to analyze the request. Probe images will not be retained beyond privacy policy guidelines. No other images will be retained by IIFC. All images and results will be provided to the originating agency for their retention.

- Face recognition search results may be saved within the entity's system audit log for audit purposes only. The audit log is available only to the Executive Director, Assistant Director, Director of Operations and Director of Intelligence and Analysis. Face recognition searches cannot be performed using the audit log.

Accountability and Enforcement

- The IIFC will follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually, and a record of the audits will be maintained by the Privacy Officer, of the IIFC pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the IIFC
- The Assistant Director**,** will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

Enforcement

If IIFC personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the Executive Director of the IIFC will:

- Suspend or discontinue access to information by the IIFC entity personnel, the participating agency, or the authorized user.
- Apply appropriate disciplinary or administrative actions or sanctions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

{Page Intentionally left blank}

Appendix A—Glossary of Terms and Definitions

The following is a list of terms and definitions used within the policy or provided for the purpose of enhancing the reader's understanding of the topics discussed.

Access—Information access is being able to get to particular information on a computer (usually requiring permission to use). Web access means having a connection to the internet through an access provider or an online service provider.

Access Control—The mechanisms for limiting access to certain information, based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role- or user-based.

Acquisition—The means by which an entity obtains face recognition information through the exercise of its authorities.

Agency—See Participating Agency.

Algorithm—An algorithm is a procedure or formula for solving a problem, based on conducting a sequence of specified actions. A computer program can be viewed as an elaborate algorithm. Algorithms can perform calculation, data processing, and automated reasoning tasks and are widely used throughout all areas of information technology.

Analysis—Refer to Image Analysis.

Attributes—Physical characteristics, such as gender, race, age, hair color, etc. that can be applied to a face recognition search.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail, such as what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security and used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provides a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, a computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, a computer process, or a device requesting access that is verified through authentication. See Authentication.

Automated Face Recognition (AFR)—Automated face recognition (AFR) software compares patterns within the field of computer vision. Such approaches do not rely upon intrinsic models of what a face is, how it should appear, or what it may represent. In other words, the matching is not based on biological or anatomical models of what a face–or the features that make up a face—look like. Instead, the algorithm

performance is entirely dependent upon the patterns which the algorithm developer finds to be most useful for finding similarities. The patterns used in AFR algorithms do not correlate to obvious anatomical features such as the eyes, nose or mouth in a one-to-one manner, although they are affected by these features.

Biometric Template—A biometric template is a set of biometric measurement data [or features] prepared by a face recognition system from a face image.[1] The prepared set can be compared to a probe image. An enrolled image, on its own, is not a biometric template. See Features.

Biometrics—A general term used alternatively to describe (1) a characteristic or (2) a process—(1) a measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition or (2) automated methods of recognizing an individual based on measureable biological (anatomical and physiological) and behavioral characteristics.[2]

Candidates—See Candidate Images.

Candidate Images—The possible results of a face recognition search. When face recognition software compares a probe image against the images contained in a repository (See Repository.), the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to or most likely resemble the probe image to warrant further analysis. A candidate image is an investigative lead only and does not establish probable cause to obtain an arrest warrant without further investigation.

Candidate List—One or more most likely candidate images resulting from a face recognition search. See Candidate Images.

Center—See Fusion Center.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.[3] They are the freedoms that are guaranteed by the Bill of Rights—the first 10 amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal- or state- protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[4]

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

Comparison—The observation of two or more faces to determine the existence of discrepancies, dissimilarities, or similarities.[5] See Face Comparison.

Computer Security—The protection of information technology assets through the use of technology, processes, and training.

Confidentiality—Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies. See Privacy.

Consent—In general use, consent means compliance in or approval of what is done or proposed by another; specifically, the voluntary agreement or acquiescence by a person of age or with requisite mental capacity who is not under duress or coercion and usually who has knowledge or understanding. Related to mobile

[1] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

[2] Ibid.

[3] *Civil Rights and Civil Liberties Protections Guidance*, at 4 (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.

[4] The definition of "civil rights" is a modified version of the definition contained in the *National Criminal Intelligence Sharing Plan* (NCISP), at pp. 5–6. *Civil Rights and Civil Liberties Protections Guidance* (August 2008), https://www.dni.gov/files/ISE/documents/DocumentLibrary/Privacy/CR-CL_Guidance_08112008.pdf.

[5] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

face recognition, consent means an individual agrees to have his or her image taken by a law enforcement officer for purposes of identification. See Revocation.

Continuous Monitoring—A system security process that comprises ongoing situational awareness of information security, vulnerabilities, threats, and incidents for each user level to support entity risk management decisions.

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are usernames, passwords, smart cards, and certificates.

Criminal Activity—A behavior, an action, or an omission that is punishable by criminal law.

Criminal Case Support—Administrative or analytic activities that provide relevant information to law enforcement personnel regarding the investigation of specific criminal activities or trends or specific subject(s) of criminal investigations.

Criminal Intelligence Information—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for a purpose other than authorized purposes. An entity's response to a data breach may be addressed in state law or agency policy. This may include incidents such as:

- Theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted.
- Posting such information on the internet.
- Unauthorized employee access to certain information.
- Moving information to a computer otherwise accessible from the internet without proper information security precautions.
- Intentional or unintentional transfer of information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail.
- Transfer of information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Data Quality—Refers to various aspects of the information, such as the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See Appendix B for a full set of FIPPs.

Direct Face Recognition Collection—The entity is owner of the face recognition equipment that captures face recognition information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Dissemination—See Disclosure.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disc optical media, or cloud technologies.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as movement of information from one location to another by magnetic or optical media, or transmission over the internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Enhancement—Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, removing noise, sharpening or brightening an image may make it easier to identify key features.

Enroll—The process of storing and maintaining information. Specifically in the face recognition context, biometric enrollment is capturing a face image, creating a biometric template from the image, and entering the template into a face recognition repository.[6] See Biometric Template and Repository.

Enrolled Image—An image that is loaded to, and may be stored in, an image repository (see Repository) and used as a reference image for face recognition comparisons (searches). Enrolled images do not include probe images. Some images of individuals may not be enrolled because they do not meet established criteria.

Enrollment—See Enroll.

Entity—The **[name of entity],** which is the subject and owner of the face recognition policy.

Evaluation—Refer to Image Evaluation.

Examiner—An individual who has received advanced training in the face recognition system and its features. Examiners have at least a working knowledge of the limitations of face recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for face recognition searches and to perform one-to-many and one-to-one face image comparisons.

Examiners determine if probe images are suitable for face recognition searches, and may enhance images for the purpose of conducting a face recognition search. Though enhancements to the probe image are permissible, the examiner does not base any conclusions on a comparison between an enhanced probe image and a potential candidate photo. Examiners shall evaluate search results by comparing the original unknown probe image with the potential candidate photo.

Expression—Facial aspects resulting from muscle movement or position.[7]

Face Comparison—The manual examination of the differences and similarities between two face images or a live subject and a face image (one-to-one) for the purpose of determining if they represent the same or different persons.[8] See Face Recognition, One-to-One Face Image Comparison, and Verification.

Face Detection—Automated determination of the locations and sizes of human faces in digital images.[9]

Face Examiner—See Examiner.

Face Recognition—The automated searching for a reference image in an image repository (see Repository) by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search). A face recognition search will typically result in one or more most likely candidates—or candidate images—ranked by computer-evaluated similarity or will return a negative result. See Candidate Images.

Face Recognition Program—An entity's face recognition initiative that includes the management of human components (management, analysts, examiners, authorized users), ownership and management of the face recognition system (technical components), and the establishment and enforcement of entity-wide processes, policies, and procedures. See Face Recognition System.

Face Recognition Software/Technology—Third-party software that uses specific proprietary algorithms to compare facial features from one specific picture—a probe image—to many others (one-to-many) that are stored in an image repository (see Repository) to determine most likely candidates for further investigation. See Candidate Images.

Face Recognition System—The technical components of a face recognition program, such as hardware, software, interfaces, image repositories, biometric templates, autogenerated candidate lists, etc. While some entities own such a system, others may only have authorized access to another entity's face recognition system. See Face Recognition Program.

Facial Recognition—See Face Recognition.

Fair Information Practice Principles—The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy

[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.

laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as entities do not generally engage with individuals and under federal law, the Privacy Act of 1974 contains exemptions in the law enforcement context. That said, law enforcement entities and all other integrated justice systems should endeavor to apply FIPPs where practicable and ensure compliance with applicable law.

The eight principles are:
1. Purpose Specification
2. Data Quality/Integrity (See definition.)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (See definition.)
6. Accountability/Audit
7. Openness/Transparency
8. Individual Participation

See Appendix B for one description of how the U.S. Department of Homeland Security applies these principles.

Features—Observable class or individual characteristics. The components of biometric templates. [10]

Filtering—In the face recognition context, filtering uses relevant physical facial attributes such as eye color, nose shape, eyebrow position, hairline, and other attributes to compare, select, and narrow results. See Attributes.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Frontal Pose—A face image captured from directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.[11]

Fusion Center—A fusion center is a collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity.[12] State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between federal and SLTT government agencies and private-sector partners.

Holistic Comparison—The process of comparing faces by looking at the face as a whole and not the component parts in isolation.[13]

Identity—Within a biometric system, the collective set of biographic data, images, and biometric templates assigned to one person.[14] See Face Comparison.

Image—See Probe Image and Repository.

Image Analysis—The assessment of an image to determine suitability for comparison, including the ability to discriminate significant features.[15]

Image Enhancement—See Enhancement.

Image Evaluation—Ascertaining the value of dissimilarities and similarities between two face images, where an examiner assesses the value of the details observed during the analysis and comparison steps and reaches a conclusion.[16]

Image Repository—See Repository.

Individual Characteristics—Characteristics allowing one to differentiate between individuals having the same class of characteristics (e.g., freckles, moles, and scars).[17]

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Individualization—The determination by an examiner that there is sufficient agreement in the quality and quantity of detail to conclude that two

[10] Ibid.
[11] Ibid.
[12] ISE-SAR Functional Standard, version 1.5.5. Source: Section 511 of the 9/11 Commission Act.
[13] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.
[14] Ibid.
[15] Ibid.
[16] Ibid.
[17] Ibid.

images depict the same person.[18] Such results are generally referred for peer and supervisory reviews and approval before any dissemination of results is made.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, including investigative information; tips and leads data, including suspicious activity reports; and criminal intelligence information.

Information Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Information Quality (IQ)—Refer to Data Quality.

Information Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the Information Sharing Environment (ISE) is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies, federal agencies, and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Intelligence—See Criminal Intelligence Information.

Invasion of Privacy— Intrusion on an individual's solitude or into an individual's private affairs, public disclosure of embarrassing private information, publicity that puts an individual in a false light to the public, or appropriation of an individual's name or picture for personal or commercial advantage. See also Right to Privacy.

Investigative Lead—Any information which could potentially aid in the successful resolution of an investigation, but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Known Image—The image of an individual associated with a known or claimed identity and recorded electronically or by other medium (also known as exemplars).[19] Known images are enrolled and stored in an image repository. See Repository.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement (LE) Agency—An organizational unit, or subunit, of a local, state, federal, or tribal government with the principal functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws. LE agencies further investigations of criminal behavior based on prior identification of specific criminal activity with a statutory ability to perform arrest functions.

Law Enforcement Information—For purposes of the ISE (see Information Sharing Environment), law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including, but not limited to, information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system which ensures that information is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases or repositories) and nonelectronic storage systems (for example, filing

[18] Ibid.

[19] Ibid.

cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Manual Face Examination—Comparison and evaluations of the probe image and the candidate images by a trained biometric images specialist.

Match/Matching—For the purposes of face recognition, see Candidate Images.

Morphological Comparison—The direct comparison of class and individual face characteristics without explicit measurement.[20] See Comparison and Manual Face Examination.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

Nodal Points—Measurements of distinctive face characteristics, including, but not limited to, the distance between the eyes, width of the nose, and the depth of the eye sockets. Nodal points are extracted from the face image and are transformed through the use of algorithms into a unique file called a biometric template. See Biometric Template.

No Match—A negative result from a face recognition search in which the probe image was determined not to be sufficiently similar to or resemble any of the reference images contained in an image repository.

Non-Criminal Justice Agency—An entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

One-to-Many Face Image Comparison—The process whereby a probe image from one subject is compared with the features of reference images contained in an image repository, generally resulting in a list of most likely candidate images (one-to-many). See Candidate Images.

One-to-One Face Image Comparison—The process whereby a probe image from one subject is compared with a most likely candidate image that is also from one subject (one-to-one). See Comparison, Face Comparison, and Verification.

Participating Agency—An organizational entity that is authorized to contribute images and/or biometric information to a face recognition system and/or is authorized to access or receive, request, or use face recognition information from the **[name of entity]**'s face recognition system for lawful purposes through its authorized individual users. Participating agencies adhere to conditions defined in a formal agreement (e.g., MOU or interagency agreement) between the **[name of entity]** operating the face recognition program and the participating agency.

Peer Review—An additional layer of verification of face recognition results in a face recognition search process. Examiners submit face recognition search results to other authorized and trained examiners—or peers—for an independent review and cross-verification of the probe and most likely candidate images. If verified by peer(s), this step is generally followed by a supervisor's review and approval prior to dissemination. Refer to Verification.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personally Identifiable Information (PII)—
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual." [21]

Pose—The orientation of the face with respect to the camera, consisting of pitch, roll, and yaw. Common poses are frontal and profile.[22]

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the

[20] Ibid.

[21] For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

[22] Ibid.

capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); and to avoid being seen or overheard in particular contexts.

Privacy Policy—Short term for a privacy, civil rights, and civil liberties (P/CRCL) policy which is a printed, published statement that articulates the policy position of an organization on how it handles the PII that it gathers or receives and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the FIPPs. The purpose of the P/CRCL policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed P/CRCL policy uses justice entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Probe Image—Any face image used by face recognition software for comparison with the face images contained within a face image repository. See Repository.

A front-facing image of an individual lawfully obtained pursuant to an authorized criminal investigation. Examples of probe images include:

- Face images captured from closed circuit TV cameras
- Face images captured from an ATM camera
- Face images provided by a victim or witness of a crime
- Face images gained from evidence (fraudulent bank card or photograph ID)
- Face sketches (for example, police artist drawings)

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instrument.

For state, local, tribal, and territorial governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, tribal, and territorial laws, ordinances, and codes. Protection may be extended to other individuals and organizations by a law enforcement entity or other state, local, tribal, or territorial agency policy or regulation.

Public—Includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, who assist the entity in the operation of the justice information system.
- Public entities whose authority to access information collected or received and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Purge—A term that is commonly used to describe methods that render data unrecoverable in a storage space or destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (e.g., made inaccessible except to system administrators or other privileged users).

Recognition—See Face Recognition.

Record—Any item, collection, or grouping of information that includes PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding

protected information about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Protected information includes personal information about individuals that is subject to information privacy or other legal protections by law. Protection may also be extended to organizations by entity policy or state, local, tribal, or territorial law.

Relative Frequency—How often facial features or combinations thereof occur in a given population.[23]

Repository—A location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a face recognition search process whereby a probe image is used by face recognition software for comparison with the images (or features within images) contained in the image repository.

Request—A request received by the **[name of entity]** to utilize face recognition in support of a criminal investigation. Submissions will not contain original evidence. Images received in a request or submission will not be stored as enrolled images within the face recognition system.

Retention—See Storage.

Revocation—In general use, revocation is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing. As it relates to the revocation of consent to be photographed or the individual's image captured by a law enforcement officer to perform a mobile face recognition search for purposes of identification, once consent to capture an individual's image is given, an individual may withdraw consent with an unequivocal act or statement of withdrawal. Consent may be withdrawn by statements, actions, or a combination of statements and actions. However, the revocation of consent must clearly be a statement revoking consent; an expression of impatience or dislike is not sufficient to terminate consent.

Revoke—See Revocation.

Right to Information Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating an individual's privacy.

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized government function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity, or the roles and responsibilities of particular personnel in the course of their official duties.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

Search—For the purposes of face recognition, the act of comparing a probe image against an image repository.[24] See Repository.

Search Filters—See Filtering.

Search Result Set—The candidate list returned from a face recognition search.[25] See Candidate Images.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information for the legitimate user set, as well as promoting failure resistance in the electronic systems overall. Security safeguarding of information is a Fair Information Practice Principle (FIPP). See Appendix B.

Source Entity—Refers to the entity or organizational entity that originates face recognition information.

Storage—In a computer, storage is the place where data is held in electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-

[23] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

[24] Ibid.

[25] Ibid.

computer storage. This is probably the most common meaning in the IT industry.

- In more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called "random access memory," or RAM) and other built-in devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations. Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

Submission—See Request.

System Bias—Errors repeatedly introduced through automation (e.g., errors in biometric template generation or comparison). Errors repeatedly introduced through operational practices in an organization or unit (e.g., improper lighting or camera position guidance).[26]

Template—See Biometric Template.

Uncontrolled Image—An image for which the subject did not pose (e.g., security camera images, cell phone photograph taken by a witness).

Unsolved Image File—A lawfully obtained probe image of an unknown suspect *may* be added by authorized law enforcement users to an unsolved image file pursuant to an authorized criminal investigation and if a search has produced no candidates and the subject remains unknown. Images in an unsolved image file are periodically compared with the known images in an image repository. Images enrolled in an unsolved image file should be required to be validated periodically by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation.

User—An **[name of entity]** employee or an individual representing a participating agency who is authorized and trained to access and use, or receive results from, an entity's face recognition system for lawful purposes.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.[27] Similar terms include "reasonable law enforcement purpose,"[28] "legitimate law enforcement purpose," and "authorized law enforcement activity."[29]

Verification—In a biometric system, the process of conducting a one-to-one comparison. A task where the face recognition system attempts to confirm an individual's claimed identity by comparing the biometric template generated from a submitted face image with a specific known template generated from a previously enrolled face image.

A review and independent analysis of the conclusion of another examiner.[30]

---

[26] Ibid.

[27] See *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, Global, BJA, OJP, DOJ, February 2013, https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations- and also in the *Real-Time and Open Source Analysis (ROSA) Resource Guide*, Criminal Intelligence Coordinating Council (CICC), Global, BJA, OJP, DOJ, July 2017, https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide (using "valid law enforcement purpose").

[28] *Recommendations for First Amendment-Protected Events for State and Local Law enforcement Agencies*, CICC, Global, OJP, DOJ, and DHS, December 2011, https://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies.

[29] The term "authorized law enforcement activity" is used, for example, in *The Attorney General's Guidelines For Domestic FBI Operations*, as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333, September 29, 2008.

[30] Glossary, FISWG, Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.